

James R. Kennedy, PhD
PO Box 1939
Hilo HI 96721-1939

Federal Communications Commission

Date: July 4, 2013

Electronic Comment Filing System RE: Supporting RM-11699, with a Further Suggestion on
Washington DC Encryption of Sensitive Emergency Communications

To Whom it May Concern:

I am a resident of the Island of Hawai'i, and also a longtime amateur radio operator (K6MIO, Extra Class). It is important to note that, here in "paradise", our geographical and geological circumstances are such that we are very vulnerable to tsunamis, earthquakes, hurricanes, lava flows, and a variety of other threats, both natural and manmade.

In a large scale disaster, the nearest airports or seaports *outside* the State are some 2,500 miles away. The airlift time is more than five hours (weather permitting) and the sealoft time is more than five days (again weather permitting). So, when something bad happens, we have to be prepared to take care of ourselves for some time until outside help can arrive. As a result, our communities are strongly dependent on the Amateur Radio Service for vital internal and external communications in times of emergencies.

I am also a member of a small volunteer community team, recruited by the County of Hawai'i (that is, the Island of Hawai'i) Civil Defense Agency, to raise the emergency communications engagement and training of our amateur radio operators to a new level. The result will be a volunteer Auxiliary Communications Service (ACS), such as are found in many continental US communities. The ACS will be an integral part of the Civil Defense Agency's emergency response program, activated by the Agency as needed, to support the County's emergency services, FEMA sponsored Community Emergency Response Teams (CERTs), and statewide Civil Defense.

RM-11699 Concept: The Need

Although I will propose an important modification in Petitioner Rolph's language, I am strongly in favor of the *concept* of RM-11699. That is: granting an exception to Part 97.113 in a declared emergency, and allowing amateur radio operators to use encryption methods to protect sensitive information required to respond to the emergency, or a recognized emergency training exercise.

It's important to note that, in a real emergency, there are a number of known circumstances that can make the use of open language over the airwaves a real problem.

HIPAA

Medical Privacy – Perhaps the most *obvious* issue is maintaining the confidentiality of individuals' personal medical information, as required by HIPAA. It is a standard practice here in Hawai'i, and in many places in the continental US, to establish, maintain, and use amateur radio stations in healthcare facilities to deal with the overloading of normal communications circuits during an emergency. Amateur radio has available forms of digital communication that could easily provide encryption of medical information in these circumstances.

Similarly, field medical stations operated by CERTs or agency first responders, and even isolated responders doing emergency first aid in the field, will all encounter the need to transmit medical information, which could be addressed by readily available digital encryption technologies.

TACTICAL ISSUES

Protecting Emergency Assets and Staff – In a major disaster (even in a small isolated place that might not make the national headlines), maintaining the civil peace can be a major issue. Experience has shown, and as Petitioner Rolph aptly points out, protecting information about the logistics of vital emergency supplies (water, food, medical materials, fuel, personnel, etc.) can be critical to ensuring that the emergency agencies can manage their distribution with the maximum effect, and reduce the threat of attempts (violent or otherwise) to purloin those supplies.

Interference With Emergency Operations – This is the “ambulance chaser” problem. One of the key issues in almost any emergency is to maintain open access for emergency services to reach the critical areas involved. Avoiding attracting a crowd of onlookers with scanners by encrypting communications about these locations would prevent major problems in serving the community.

Avoiding Panic – In an emergency, communications with the public is a two-way street. People in the effected areas are not only anxious to be heard, they are also very concerned about when their needs will be met and, in general, “what’s happening”. The issue is that it takes *time* to size up any complex emergency situation, and be able to ensure the public is accurately informed.

Unfortunately, at the outset, as responders are trying to piece together the facts of the situation, inevitably there will be conflicting and inaccurate information flying about the airwaves. Again with the scanners in mind, this can cause the general public unnecessary confusion, anxiety, and even panic. The emergency management agencies already have the option of limiting this risk by encrypting *their* communications during this process. Since amateur radio operators are *also key sources* of the management agency’s needed size-up information, it would be important that they also could use the encryption option, when so directed by the relevant emergency agency.

NATIONAL SECURITY

Sadly, it seems there is a growing number of emergencies with national security implications. Since the amateur radio operators will be in the field doing basically the same job as the emergency agency staff, encryption should be an option.

Important Proposed Modification of the RM-11699 Language

While I am in broad agreement with Petitioner Rolph’s suggestion, I must respectfully point out that, requiring “*Federal authorities managing relief and training efforts*” to designate which data is to be encrypted, simply will ***not*** work when a disaster is actually occurring, because:

Boots-on-the-ground, real-time emergency management is ***not done*** by a *Federal authority*.

It is almost always managed by state, county, or city level authorities that are, by law, formally charged with this responsibility, and are already in place, and most aware of the community needs and the immediately available resources. This is a Constitutional reality, and a very practical one. It is not a Federal authority that tells a state, county, or city what to do in real time

in a civil emergency. *Quite the reverse*, typically it is the *state* authority that requests Federal help, when it is needed. In the most critical acute phase of an emergency, the local authorities have to be in charge in order to even determine if Federal assistance is needed, and what that assistance might be.

When Federal "management" is involved, frequently it is in a supporting role providing supplies, personnel, and later on, assistance in restoring and rebuilding infrastructure. It is not normally about real-time search and rescue, and immediate crisis mitigation.

The main point is that it is critical that the language be structured so that the actual real-time responsible authority, at *any* phase of the emergency response, have the say as to when, and which, data is to be encrypted, – whether it is a state, county, city, or Federal agency.

I am not an attorney, but I believe that the language should be rephrased as something like:

(c) intercommunications when participating in emergency services operations or related training exercises which may involve information covered by HIPAA or other sensitive data such as logistical information concerning medical supplies, personnel movement, other relief supplies or any other data designated by Federal *the responsible emergency* authorities managing the relief or training effort."

Final Comments

I would also point out that there is a very close relationship between the motivation for the two *existing exceptions* to the Part 97.113 prohibition of encrypted transmissions, and the spirit of the RM-11699 petition.

The exception for command and control of space stations in the amateur satellite service and the command and control of unattended amateur radio stations are basically motivated by the desire to ensure that valuable communications assets are not destroyed, damaged, or perverted for unauthorized usage. The current petition is motivated by the very same concerns, except that the circumstances are far more critical. Here, the lives, welfare, and property of the public are, and will be, at stake.

With my thanks to Petitioner Rolph for shining a light on this important issue, respectfully submitted,

A handwritten signature in dark ink, appearing to read 'J.R. Kennedy', with a stylized flourish at the end.

James R. Kennedy, PhD